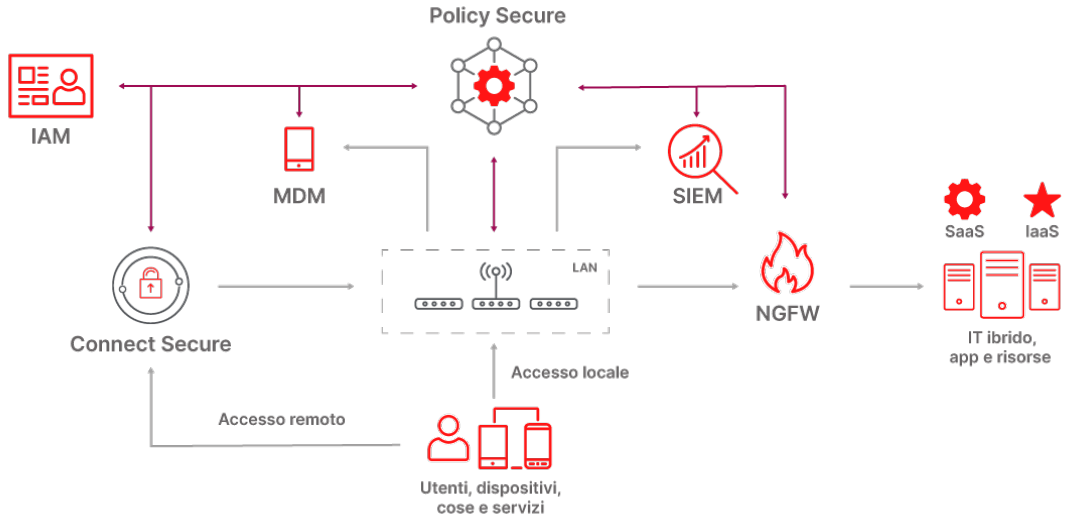
Difesa integrata contro le minacce con Policy Secure

Panoramica

Per proteggere i dati e le risorse, il personale della sicurezza aziendale utilizza soluzioni come i Firewall di prossima generazione (NGFW) per controllare l'accesso e monitorare i flussi di traffico, e i Security Information and Event Manager (SIEM) per analizzare e correlare gli eventi. Il problema è che queste soluzioni sono limitate all'invio di avvisi o all'applicazione di politiche sul traffico che le attraversa. Le soluzioni Network Access Control (NAC) tradizionalmente applicano la postazione di sicurezza di un endpoint prima di connettersi alla rete. L'integrazione bidirezionale con l'ecosistema di sicurezza permette a un NAC di aumentare l'efficacia complessiva della sicurezza prendendo misure correttive sulla connettività di un endpoint dopo aver ricevuto avvisi da altre soluzioni di sicurezza. L'applicazione automatica della sicurezza con un NAC fornisce dei benefici che includono:



- Riduzione del tempo di risposta alle minacce.
- Operazioni di sicurezza semplificate.
- Limitazione della diffusione laterale delle minacce.
- Conformità della sicurezza automatizzata e audit più facili.
- Politiche più granulari con informazioni contestuali.

Policy Secure si integra con i dispositivi dell'infrastruttura di rete e di sicurezza come gli switch, i controller wireless e i firewall di nuova generazione (NGFW), ma anche con soluzioni come la gestione delle identità e degli accessi (IAM), SIEM, Advanced Threat Protection (ATP) e Enterprise Mobility Management (EMM). Policy Secure permette decisioni di accesso automatizzate e attivabili basate su dati contestuali come l'identità, la postazione di sicurezza e la posizione. Basato su una struttura di accesso a fiducia zero, Policy Secure applica continuamente il livello di fiducia di un endpoint durante il suo ciclo di vita della connettività e lo mette in quarantena quando viene rilevata un'anomalia comportamentale.

Integrazioni per la valutazione continua della fiducia

Accesso alla rete

Il principio della fiducia zero: verificare sempre. Policy Secure convalida prima l'utente e il dispositivo rispetto alla politica. Quindi, Policy Secure connette il dispositivo con l'infrastruttura di accesso in linea con il ruolo dell'utente. Questa segmentazione dinamica della rete limita la diffusione laterale delle minacce tra diverse classi di dispositivi IoT e utenti.
PPS si integra con le principali soluzioni di switching e Wi-Fi di fornitori come Cisco, Juniper, Mist, Aruba, Huawei e Ruckus utilizzando lo standard comune 802.1X o SNMP.

Il provisioning dinamico del perimetro di rete fornisce un altro livello di controllo dell'accesso. Le politiche NGFW possono sfruttare informazioni contestuali aggiuntive come l'identità o la posizione dell'utente. PPS si integra con le soluzioni NGFW come Palo Alto Networks, Checkpoint, Juniper e Fortinet, per fornire queste informazioni contestuali sull'endpoint.

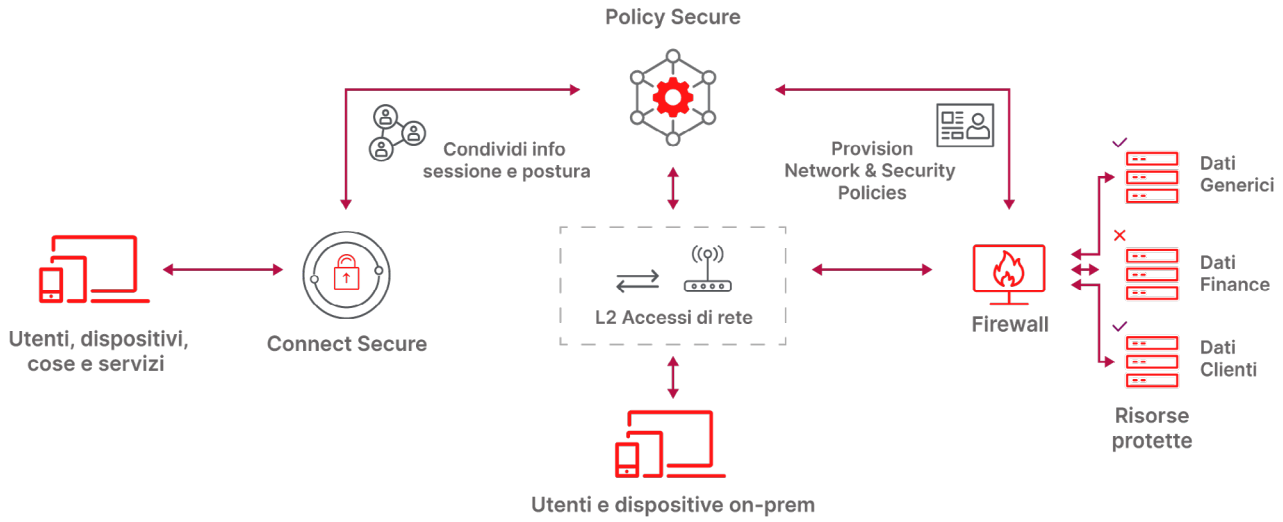
Conformità degli endpoint

Gli endpoint utilizzano un'ampia varietà di software tra cui il sistema operativo, le utility di sicurezza come l'antivirus e le applicazioni a livello utente. Tutto questo software riceve aggiornamenti periodici per i miglioramenti delle funzioni e le correzioni di sicurezza. La funzione di controllo dell'host valuta continuamente la postazione di sicurezza del dispositivo convalidando la cronologia degli aggiornamenti software e le applicazioni attive.
Una volta che Policy Secure concede l'accesso alla rete ad un utente e/o ad un dispositivo, monitora continuamente la postazione di sicurezza durante tutto il ciclo di vita della connettività. Se la postazione di sicurezza cambia, per esempio perché l'utente lancia un'applicazione shadow IT che viola la politica, Policy Secure sposta immediatamente l'endpoint in un ambiente di rete limitato.

Policy Secure aiuta le organizzazioni a minimizzare i rischi applicando automaticamente la conformità dell'endpoint. Il controllo degli host può interagire con Windows Management Instrumentation, Windows Defender, Microsoft Security Essentials o il client VPN Connect Secure di Ivanti per una maggiore granularità.

Gestione dell'identità e dell'accesso (IAM)

Il meccanismo di autenticazione convalida l'identità di un utente e definisce i ruoli. Il sistema può sfruttare le informazioni contestuali basate su tempo, geolocalizzazione o comportamento. Per esempio, se esistono già sessioni autenticate in una diversa geolocalizzazione, l'utente può essere sottoposto a metodi di autenticazione aggiuntivi come l'autenticazione a due fattori (2FA). Policy Secure si integra con le soluzioni IAM utilizzando protocolli come SAML (Ping, Okta, Duo ecc.), Active Directory (Microsoft), o anche RADIUS/TACACS+ o LDAP per ambienti più isolati. Policy Secure viene fornito con un servizio RADIUS integrato.



Eventi di sicurezza

Una strategia di sicurezza solida e stratificata richiede l'analisi continua dei flussi di rete e degli eventi, utilizzando soluzioni come Firewall di prossima generazione (NGFW), Security Information and Event Management (SIEM) o Advanced Threat Detection (ATD). L'integrazione bidirezionale con Policy Secure migliora l'efficacia complessiva della sicurezza con risposte automatiche e attuabili a livello di accesso alla rete. Le risposte automatizzate agli Indicatori di Compromissione (IoC) riducono il tempo di riparazione e ottimizzano le risorse amministrative.

PPS si integra con i principali NGFW, come Palo Alto Networks, Checkpoint, Juniper e Fortinet, così come con soluzioni SIEM come IBM QRadar e Splunk.

Caso d'uso: Allarme NGFW

Quando un NGFW scopre una minaccia, avvisa Policy Secure, utilizzando il syslog standard. Policy Secure può mettere in quarantena il dispositivo sospetto in un ambiente ad accesso limitato per risolvere il problema e prevenire la diffusione laterale della minaccia.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com